1.- 6.   (Canceled)

7.   (Currently amended)   A method wherein an account issuer authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said third party desiring verification as to the identity of said customer before proceeding with said online transaction with said customer, said method comprising:

receiving, by said issuer, authentication information concerning said customer;

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

receiving a verify enrollment request message at an access control server operated by said issuer during said online transaction as to whether said customer account is registered;

sending a verify enrollment response message back to said third party indicating that said customer account is registered;

receiving an authentication request message at **said** ~~an~~ access control server ~~operated by said issue~~r from said third party during said online transaction, said message requesting verification of the identity of said customer, said **authentication** request message being routed via an Internet browser of a computer of said customer **and being sent after said verify enrollment response message**;

requesting over a network, by said issuer from said customer during said online transaction, of an identity-authenticating password;

verifying, by said issuer, that said identity-authenticating password from said customer matches said password previously designated for said account; and

notifying said third party over said network during said online transaction, by said issuer, that said customer is the actual owner of said account when said identity-authenticating password entered by said customer matches the password that was previously designated for said account,

said notifying being routed via said Internet browser of said computer of said customer, ~~said method not requiring use of any additional software on said computer of said customer,~~ whereby said issuer authenticates said customer for said third party during said online transaction.

8.   (Previously presented)   A method as recited in claim 7 wherein said issuer is an issuer financial institution and said third party is an online merchant, whereby said online merchant conducts an online financial transaction with said customer, and wherein said account of said customer is maintained by said issuer financial institution.

9.   (cancelled)

10.   (Currently amended) A method as recited in **claim 7** ~~claim 9~~ wherein the access control server determines if said customer account is **registered** ~~enrolled~~ by verifying that said customer account is contained in a database of enrolled customer accounts.

11.   (Currently amended) A method as recited in **claim 7** ~~claim 9~~ further comprising:
        sending said **verify enrollment request message from said third party to** ~~querying~~ a directory server to verify that said customer account is **registered** ~~associated with an issuer financial institution that is participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution~~.

12.   (Currently amended) A method as recited in **claim 7** ~~claim 11~~ further comprising:
        including within said verify enrollment response message ~~sending to said third party's computer system~~ an Internet address for said access control server, ~~said Internet address passing through said directory server before reaching said third party's computer system,~~ whereby said Internet address for said access control server allows said third party to ~~directly~~ communicate with said access control server.

3

13.   (Currently amended)   A method as recited in **claim 7** ~~claim 9~~ further comprising:

reviewing a memory device controlled by said third party to verify that said customer account is **registered** ~~associated with an issuer financial institution participating in said payment authentication service, whereby said customer account is not enrolled with said payment authentication service if said customer account is not associated with an issuer financial institution~~.

14.   (Previously presented)   A method as recited in claim 7 further comprising:

generating, by said issuer, a digitally-signed transaction receipt using a signature key of said issuer; and

sending, by said issuer, said digitally-signed transaction receipt to said third party, whereby said digitally-signed transaction receipt confirms to said third party that the identity of said customer has been authenticated.

15.   (Previously presented)   A method as recited in claim 14 wherein said transaction receipt includes a number associated with said customer account, a transaction payment amount, and a transaction payment date.

16.   (Previously presented)   A method as recited in claim 7 further comprising:

sending, by said issuer, a card authentication verification value to said third party, the card authentication verification value containing a unique value for said customer account and a specific payment transaction, whereby said card authentication verification value uniquely identifies a specific authenticated payment transaction.

17.   (Previously presented)   A method as recited in claim 14 further comprising:

verifying, by said third party, said digitally signed transaction receipt such that said third party is assured that said transaction receipt was sent from a specific issuer.

18.   (Previously presented)   A method as recited in claim 7 further comprising:

sending, by said third party, of an authorization message to an issuer financial institution to verify said customer account has adequate credit for a requested purchase.

4

19.   (Previously presented)   A method as recited in claim 7 wherein said first step of verifying further comprising:

receiving, by said issuer, said authentication information entered at an enrollment Internet web site by said customer;

verifying, by said issuer, that said enrollment information substantially matches information contained within a pre-existing database of customer information; and

storing said customer account information in a database for enrolled customer accounts.

20.   (Currently amended)   A method performed by an authentication service wherein an account issuer authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said method comprising:

receiving, by said issuer, authentication information concerning said customer;

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

performing a verification process by said third party during said online transaction to determine whether said customer account is registered;

sending an authentication request message via a customer computer from a third-party software module over a network during said online transaction**, said request message being sent after said verification process**;

receiving said authentication request message at an access control server that is operated by said issuer;

requesting over said network, by said issuer, of a password from said customer;

verifying, by said issuer, that said password entered by said customer matches said password previously designated for said account; and

sending over said network, by said issuer, an authentication response message to a third-party software module, said authentication response message containing an authentication status indicator, said response message being routed via said computer of said customer, ~~said method not requiring use of any additional software on said customer computer,~~ whereby said issuer authenticates said customer for said third party.

21.   (Currently amended)   A method performed by a customer computer used with an authentication service wherein an issuer financial institution authenticates, for the benefit of a third party, that a customer using an account during an online transaction with said third party is the actual owner of said account, said method comprising:

sending enrollment information to an enrollment web site by said customer during a registration process so that said issuer verifies the identity of said customer as the owner of said account;

supplying a password to be designated for said account during said registration process;

performing a verification process by said third party during said online transaction to determine whether said customer account is registered with said authentication service;

receiving, by said customer computer **after said verification process**, an authentication request message from said third party during said online transaction that requests ~~the initiation of an authentication service wherein~~ the identity of said customer ~~will~~ be authenticated;

sending said authentication request message to an access control server operated by said issuer financial institution, said customer having an account with said issuer financial institution;

receiving a request from said access control server for said customer to enter a password used to verify the identity of said customer during said online transaction;

supplying said password used to verify identity; and

facilitating the sending of an authentication response message from said access control server to said third party via said customer computer regarding the verification of the identity of said customer, ~~said method not requiring use of any additional software on said customer computer,~~ whereby said access control server verifies the identity of said customer for said third party.

22. - 31.   (Canceled)

32.   (Currently amended)   A method performed by an authentication service wherein an account issuer authenticates a customer for the benefit of a third party, said method comprising:

receiving, by said issuer, authentication information concerning said customer;

verifying, by said issuer during a registration process, the identity of said customer as the owner of said account and associating a designated password with said account;

receiving a request over a network from a customer computer to perform an online financial transaction with said third party;

performing a verification process by said third party during said online transaction to determine whether ~~determining that~~ said customer **account** is enrolled in said authentication service;

sending an authentication request message from said third party via said customer computer over a network during said financial transaction, said authentication request message destined for a computer of said issuer **and being sent after said performing**;

receiving an authentication response message from said computer of said issuer via said customer computer during said financial transaction, said authentication response message indicating the authenticity of said customer, said authenticity being based upon a password supplied by said customer to said computer of said issuer during said financial transaction and upon said password previously designated for said account, ~~said method not requiring use of any additional software on said customer computer,~~ whereby said issuer authenticates said customer for said third party.

33.   (Previously presented)   A method as recited in claim 7 wherein said online transaction is a payment transaction.

34.   (Previously presented)   A method as recited in claim 20 wherein said online transaction is a payment transaction.

35. (Previously presented) A method as recited in claim 21 wherein said online transaction is a payment transaction.

36. (Previously presented) A method as recited in claim 32 wherein said financial transaction is a payment transaction.

37. (Previously presented) A method as recited in claim 20 wherein said third-party software module sends said authentication request message to said access control server by way of a browser in said customer computer, and wherein said issuer sends said response message to said third-party software module by way of said browser in said customer computer.

38. (Previously presented) A method as recited in claim 20 wherein said third-party software module sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said access control server.

39. (Previously presented) A method as recited in claim 32 wherein said third party sends said authentication request message to said issuer computer by way of a browser in said customer computer, and wherein said issuer sends said response message to said third party by way of said browser in said customer computer.

40. (Previously presented) A method as recited in claim 32 wherein said third party sends said authentication request message to a software module of said customer computer and wherein said customer computer then sends said authentication request message to said issuer computer.

41. (canceled)

42.   (Previously presented)   A method as recited in claim 7 further comprising:

accessing a web site of said third party by said customer using an Internet browser of said customer computer;

redirecting said Internet browser of said customer computer from said web site to said access control server of said issuer, whereby said issuer receives said identity-authenticating password; and

redirecting said Internet browser of said customer computer from said access control server back to said web site of said third party.

43.   (canceled)

44.   (cancelled)

45.   (Previously presented)   A method as recited in claim 7 wherein said access control server receives said customer authentication information and said designated password from said issuer during said registration process, whereby said customer need not go through a formal registration process.

46.   (Previously presented)   A method as recited in claim 7 wherein said access control server receives said customer authentication information and said designated password from said customer during said registration process, whereby said registration process is a formal registration process.

47.   (Previously presented)   A method as recited in claim 20 further comprising:

redirecting an Internet browser of said customer computer from said third party to said access control server of said issuer, whereby said issuer receives said entered password; and

redirecting said Internet browser of said customer computer from said access control server back to said third party.

48. (Previously presented) A method as recited in claim 21 further comprising:

accessing a web site of said third party by said customer using an Internet browser of said customer computer;

redirecting said Internet browser of said customer computer from said web site to said access control server of said issuer, whereby said issuer receives said password; and

redirecting said Internet browser of said computer from said access control server back to said web site of said third party.

49. (Previously presented) A method as recited in claim 32 further comprising:

performing said sending by redirecting an Internet browser of said customer computer from a web site of said third party to said computer of said issuer, whereby said issuer receives said password; and

performing said second step of receiving by redirecting said Internet browser of said customer computer from said computer of said issuer back to said web site of said third party.

50. (New) A method as recited in claim 20 wherein said performing includes

querying a directory server by said third party to determine if said customer account is within a particular range.

51. (New) A method as recited in claim 20 wherein said performing includes

directly querying said access control server by said third party.

52.   (New)   A method as recited in claim 20 wherein said performing includes

checking a cache memory of said third party.

53.   (New)   A method as recited in claim 21 wherein said performing includes

querying a directory server by said third party to determine if said customer account is
within a particular range.

54.   (New)   A method as recited in claim 21 wherein said performing includes

directly querying said access control server by said third party.

55.   (New)   A method as recited in claim 21 wherein said performing includes

checking a cache memory of said third party.

56.   (New)   A method as recited in claim 32 wherein said performing includes

querying a directory server by said third party to determine if said customer account is
within a particular range.

57.   (New)   A method as recited in claim 32 wherein said performing includes

directly querying said issuer computer by said third party.

58.   (New)   A method as recited in claim 32 wherein said performing includes

checking a cache memory of said third party.